HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10003536-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Russell et al.

Confirmation No.: 1330

Application No.: 09/838,759

Examiner: Klimach, P.

Filing Date: 04/19/2001

Group Art Unit: 2135

Title: DATA SECURITY FOR DISTRIBUTED FILE SYSTEM

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Sir:

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on **06/14/2005**.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

( ) (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d) for the total number of months checked below:

( )	one month	$120.00
( )	two months	$450.00
( )	three months	$1020.00
( )	four months	$1590.00

( ) The extension fee has already been filled in this application.

(X) (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account **08-2025** the sum of **$500.00**. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

(X) I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450. Date of Deposit: **08/11/2005**

OR

( ) I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number _____ on _____

Number of pages:

Typed Name: **Kathleen McDevitt**

Signature: Kathleen McDevitt

Respectfully submitted,

Russell et al.

By _____

LeRoy D. Maunu

Attorney/Agent for Applicant(s)
Reg. No. **35,274**

Date: **08/11/2005**

Telephone No.: **(651) 686-6633**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	Russell et al.	Examiner:	Klimach, P.
Serial No.:	09/838,759	Group Art Unit:	2135
Filed:	April 19, 2001	Docket No.:	10003536-1
Title:	DATA SECURITY FOR DISTRIBUTED FILE SYSTEM		

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence and the papers, as described hereinabove, are being deposited in the United States Postal Service, as first class mail, in an envelope addressed to: Board of Patent Appeals and Interferences, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450, on August 11, 2005.

By: Kathleen McDevitt
Kathleen McDevitt

Board of Patent Appeals and Interferences
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an Appeal Brief submitted pursuant to 37 C.F.R. § 41.37 for the above-referenced patent application.

I. Real Party in Interest

The real party in interest is Hewlett-Packard Company having a place of business at 1501 Page Mill Road, Palo Alto, CA. The above referenced patent application is assigned to Hewlett-Packard Company.

II. Related Appeals and Interferences

Appellant is unaware of any related appeals, interferences or judicial proceedings.

III. Status of Claims

Claims 1-16 are rejected and are presented for appeal. The appealed claims are in the attached Appendix of Appealed Claims.

IV. Status of Amendments

No amendment has been filed subsequent to the final rejection.

V. Summary of Invention

One embodiment of the invention provides a computer-implemented method for controlling access by a plurality of client applications (FIG. 1, #108a-b;) to file data in a distributed file system. The distributed file system includes a distributed file system interface (FIG. 1, #104a-b; p. 4, l. 27-33) coupled to the client applications and a storage server (FIG. 1, #106; p. 5, l. 1-2) and a meta-data server (FIG. 1, #102; p. 5, l. 5-10) coupled to the distributed file system interface. The method includes receiving at the meta-data server an open-file request (FIG. 1, #122). A security object is created at the meta-data server in response to the open-file request (FIG. 1, #124; p. 5, l. 25). The meta-data server and the storage server generate an encryption key and the encryption key is stored in the security object (FIG. 1, #124, #126; FIG. 2, #202; FIG. 3, #304; p.7, l. 13-23; p. 8, l. 16-17). A list that identifies the first set of blocks is encrypted (FIG. 2, #208; p. 7, l. 24-25), and the encrypted block list is added to the security object (FIG. 2, #208; p. 7, l. 24-25). The security is transmitted object to the distributed file interface (FIG. 1, #128; FIG. 2, #210; p. 7, l. 26-27).

In another embodiment, the invention provides an apparatus for controlling access by a plurality of client applications to file data in a distributed file system. The apparatus includes means for receiving (p. 5, l. 1-4) at the meta-data server an open-file request (FIG. 1, #122); means for creating (p. 5, l. 1-4) a security object at the meta-data server in response to the open-file request (FIG. 1, #124; p. 5, l. 25); means for generating (p. 5, l. 1-4) an encryption key at the meta-data server and the storage server and storing the encryption key in the security object (FIG. 1, #124, #126; FIG. 2, #202; FIG. 3, #304; p.7, l. 13-23; p. 8, l. 16-17); means for encrypting (p. 5, l. 1-4) a list that identifies the first set of blocks, whereby an encrypted block list is formed (FIG. 2, #208; p. 7, l. 24-25); means for adding (p. 5, l. 1-4) the encrypted block list to the security object (FIG. 2, #208; p. 7, l. 24-25); and means

for transmitting (p. 5, l. 1-4) the security object to the distributed file interface (FIG. 1, #128; FIG. 2, #210; p. 7, l. 26-27).

A system is provided, in another embodiment, for controlling access by a plurality of client applications to file data in a distributed file system. The system includes a distributed file system interface (FIG. 1, #104a-b; p. 4, l. 27-33) coupled to the client applications. The distributed file interface is configured to transmit open file requests to a meta-data server (FIG. 1, #102; p. 5, l. 5-10) and file access requests to a block storage server (FIG. 1, #106; p. 5, l. 1-2). The meta-data server is coupled to the distributed file system interface and to the block storage server. The meta-data server is configured to generate a partial encryption key (FIG. 1, #124, #126; FIG. 2, #202; FIG. 3, #304; p.7, l. 13-23; p. 8, l. 16-17), store the partial encryption key in a security object (FIG. 2, #204; p. 7, l. 19-21), transmit the security object to the block storage server for completion of the encryption key (p. 7, l. 19-21), encrypt a list of blocks in a file as an encrypted block list (FIG. 2, #208; p. 7, l. 24-25), and return the security object with the encrypted block list to the distributed file system interface (FIG. 1, #128; FIG. 2, #210; p. 7, l. 26-27). The block storage server (FIG. 1, #106; p. 5, l. 1-2) is coupled to the distributed file system interface and is configured to generate a complete encryption key from the partial encryption key in the security object (FIG. 3, #304; p. 8, l. 16-17), and return the security object with the complete encryption key to the meta-data server (FIG. 3, #308; p. 8, l. 21-22).

VI. Grounds of Rejection

A. Claims 1-4, 8-9, and 13-16 stand rejected under 35 U.S.C. §103(a) as being unpatentable over "Moore" (U.S. patent number 6,678,700) in view of "Moskowitz" (U.S. patent publication number 20020071556A1) and "Brundrett" (U.S. patent number 6,249,866).

VII. Argument

A. The rejection of claims 1-4, 8-9, and 13-16 should be reversed because the Examiner has not established a *prima facie* case of

obviousness of the claims under 35 U.S.C. §103(a) over Moore in view of Moskowitz and Brundrett.

The Examiner has failed to establish a *prima facie* case of obviousness of claims 1-4, 8-9, and 13-16 over Moore in view Moskowitz and Brundrett because all the limitations are not shown to be suggested by the combination, and a proper motivation for modifying Moore with teachings of Moskowitz and Brundrett has not been provided.

Claims 1, 3-4, 8-9, 13-14, 16

The Office Action fails to show that the combination suggests the limitations of claims 1, 13 and 14. For example, Moskowitz is not shown to suggest generating an encryption key at the metadata server and at the storage server and storing the key in the security object. The cited paragraph [0023] of Moskowitz discusses breaking an encryption key into partial keys. However, there is no apparent suggestion of generating a key by a met-data server and a storage server. The Examiner cites the concept of partial keys but fails to provide any evidence from the prior art that suggests generating a key by a meta-data server and a storage server. Furthermore, there no apparent suggestion of storing the key in a security object which is provided to a distributed file system interface.

Brundrett is not shown to suggest the limitations of storing the key in the security object, encrypting a list that identifies a set of blocks in the opened file, and adding the encrypted list to the security object. The Office Action cites Brundrett's teaching of an "encrypting file system driver" communicating with an "EFS service by passing it the file metadata, including the data decryption and data recovery fields" as teaching these limitations. However, there is no cited nor readily apparent suggestion that Brundrett encrypts a list that identifies a set of blocks in the opened file, nor any apparent suggestion of that Brundrett adds the encrypted list to the security object. Since Brundrett does not appear to use a distributed file system interface along with the claimed meta-data server and block storage server, Brundrett would have no apparent need to encrypt the list of blocks for transmission

back to a distributed file system interface. Furthermore, those skilled in the art will recognize the distinction between encrypting a list that identifies blocks in a file versus encrypting the file data.

The further alleged correspondences between elements of Brundrett and the claim limitations also demonstrate the failure to show that all the limitations are suggested by the prior art. The Examiner further alleges that "Brundrett discloses the key being extracted from the meta data, [from which] it can therefore be inferred that the key was stored (inserted) in the meta data (column 65, lines 15-20)." This statement seemingly conveys that the Examiner understands Brundrett's metadata as corresponding to the claimed security object. The Examiner also alleges that "since a file is a block of text that can be selected and acted upone [sic] as a whole in an application, then the directory is the list that identifies a set of blocks (column 5 lines 10-15)." Thus, the Examiner apparently understands Brundrett's directory as corresponding to the claimed block list. These alleged correspondences demonstrate that Brundrett does not suggest the claim limitations.

If Brundrett's meta data corresponds to the claimed security object and Brundrett's directory data corresponds to the claimed block list, then in order to show that all the claim limitations are suggested by Brundrett, the Examiner would need to show that Brundrett's encrypted directory data is stored in Brundrett's metadata. Not only does the Examiner fail to show this limitation, but Brundrett's FIGs. 8 and 9 appear to indicate that encrypted directory data is not stored as part of the metadata (col. 16, l. 5-22). Thus, the limitations of the claimed security object, in which both the key and the encrypted block list are stored, are not shown to be suggested by Brundrett.

The cited teachings of Moore do not suggest transmitting of the claimed security object to a distributed file interface. Moore's FIG. 7 and the teaching of a client performing a write function to an object maintained by the server is alleged to correspond to these limitations. However, no further teaching of Moore is cited to suggest any objects that correspond to or are analogous to the claimed security object. Moore's general teaching of writing to an object by a client does not suggest

the specific claim limitations of the security object being transmitted to a distributed file interface.

In addition to failing to show a suggestion of the various limitations of claims 1, 13, and 14, the Office Action also fails to provide proper motivations for combining Moskowitz with Moore and for combining Brundrett with the Moore-Moskowitz combination.

The alleged motivation for modifying Moore with Moskowitz is conclusory, based on hindsight and therefore, improper. The alleged motivation is that "it would have been obvious ... to use partial keys created at different servers as in the system of Moskowitz and adding the keys to the data portion of the object in the system of Moore, thus creating a security object ... because sharing the secret between more devices increase the amount of security since both values are required fore [sic] decrypting the message." This alleged motivation merely states a function of partial keys. No particular evidence is provided that would motivate one to modify Moore's system. Moore's system is presumably adequate for its intended purpose, and no evidence is provided to indicate any deficiencies in Moore's system. Thus, the alleged motivation is merely a reconstruction of the claim limitations based on hindsight.

The alleged motivation for modifying the Moore-Moskowitz combination with Brundrett is also conclusory, based on hindsight, and therefore, improper. The alleged motivation is "that it would have been obvious ... to encrypt the file as in Brundrett and adding the encrypted information to the data portion of the object in the system of Moore ... because encryption secures the information." This alleged motivation simply states the function of encryption. No evidence is provided to suggest that the Moore-Moskowitz combination is in any way lacking in security features. Furthermore, no evidence is presented to indicate how specific teachings of Brundrett would improve the security of the Moore-Moskowitz combination. Thus, the alleged motivation is merely a reconstruction of the claim limitations based on hindsight.

Claims 3-4 and 8-9 depend directly or indirectly from claim 1 and are thought to be patentable over the Moore-Moskowitz-Brundrett combination for at least the reasons set forth above.

Claims 13 and 14 include functional limitations similar to those of claim 1 and are thought to be patentable over the Moore-Moskowitz-Brundrett combination for at least the reasons set forth above.

Claim 16 depends from claim 14 and is thought to be patentable over the Moore-Moskowitz-Brundrett combination for at least the reasons set forth above.

Claims 2, 15

The Office Action fails to show that the limitations of claim 2 are suggested by the Moore-Moskowitz-Brundrett combination, and the alleged motivation for making the combination is improper. Claim 2 includes limitations of transmitting a file access request and security object from the distributed file system interface to the storage server in response to a file access request from a client application, the file access request including an operation code and a reference to selected data of a file; decrypting the block list at the storage server in response to the file access request; providing access to the selected data in accordance with the operation code upon successful decryption of the block list.

As explained above, the combination does not suggest the claimed security object. Therefore, there is no apparent correspondence of transmitting a file access request and the claimed security object from the distributed file system interface to a storage server. Furthermore, the Office Action cites Brundrett's decrypting of text. However, the cited col. 17 of Brundrett teaches that the file data is decrypted. There is no apparent correspondence between the claimed decrypting of the block list in the security object (which identifies a set of blocks in the file) and Brundrett's decrypting of file data. Therefore, the limitations of claim 2 are not shown to be suggested by the Moore-Moskowitz-Brundrett combination.

The alleged motivation for modifying the Moore-Moskowitz combination with the cited teachings of Brundrett is improper because it is conclusory and based on hindsight. The alleged motivation states that "it would have been obvious ... to

decrypt the file as in Brundrett in the system of Moore ... because decryption makes the encrypted data available to the user." This alleged motivation simply states a function of decryption without providing any evidence to indicate that the Moore-Moskowitz combination, which presumably decodes data (Moskowitz Abstract), has any further need for or would benefit from Brundrett's decryption. Therefore, the alleged motivation is simply a hindsight based reconstruction of the invention.

Claim 15 includes functional limitations similar to those of claim 2 and is thought to be patentable over the Moore-Moskowitz-Brundrett combination for at least the reasons set forth above.

VIII. Conclusion

Claims 5-7 and 10-12 were deemed allowable if rewritten to include the limitations of the base claims and any intervening claims. These claims remain as originally filed because the base claims are thought to be patentable over the Moore-Moskowitz-Brundrett combination.

In view of the above, Appellant submits that the rejections are improper, the claimed invention is patentable, and that the rejections of claims 1-16 should be reversed. Appellant respectfully requests reversal of the rejections as applied to the appealed claims and allowance of the entire application.

Respectfully submitted,

CRAWFORD MAUNU PLLC
1270 Northland Drive, Suite 390
Saint Paul, MN 55120
(651) 686-6633

By: 
Name: LeRoy D. Maunu
Reg. No.: 35,274